Vanessa das Neves Pimentel

<Métodos de criptografia para sinais de voz>

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica e de Telecomunicações da Universidade Federal Fluminense como requisito parcial para a obtenção do Grau de Mestre em Engenharia Elétrica e de Telecomunicações. Área de concentração: Sistemas de Telecomunicações.

Aprovada em maio de 2016.

BANCA EXAMINADORA

Prof. Edson Cataldo - Orientador, UFF

Prof. Wanderley Rezende, UFF

Prof. Leonardo Forero Mendoza, UERJ

Prof. Natalia Castro Fernandes, UFF

Niterói

2016

Dedicatória: Para Cacilda (In memoriam) e Leandro.

Agradecimentos

Primeiramente agradeço a Deus por mais uma etapa concluída em minha vida.

À minha mãe Cacilda (*in Memorian*), agradeço pelo amor incondicional, os ensinamentos, a ajuda nas escolhas mais importantes da minha vida e o incentivo a crescer e me tornar o que sou hoje.

Ao meu marido Leandro, por todo amor e carinho, apoio, ajuda nos momentos mais difícies, pelas palavras sábias e calmas, e principalmente o incentivo durante esta caminhada.

Aos meus amigos Nathália, Renata, Paola, Marly, Rodrigo e Thiago e a minha irmã Bianca, por serem tão especiais na minha vida, me entenderem nos momentos mais difíceis e me perdoarem pelas ausências.

Aos meus familiares, especialmente minha avó Maria, Cirleia (*in Memorian*), Bárbara, Erika, Jorge, Renan, Kainan e meus afilhados Júlia e Arthur, por me apoiarem e entenderem que nem sempre estamos perto de quem amamos.

Ao meu orientador Edson Cataldo, pela oportunidade, ajuda, contribuição, orientação, confiança e disponibilidade ao longo desta etapa.

À CAPES pelo suporte financeiro.

Ao Curso de Pós-Graduação em Engenharia Elétrica e de Telecomunicações da Universidade Federal Fluminense pela oportunidade de aumentar meus conhecimentos.

Aos professores que fizeram e fazem parte da minha vida e que de alguma forma contribuíram para o meu conhecimento. Em especial, o professor Wanderley Rezende, pelo incentivo desde a epóca da graduação e pela confiança demonstrada, a professora Natalia Castro, pela disponibilidade e o apoio durante o mestrado, e aos professores Marcia Cerioli e Petrucio Viana, por me entenderem e me ajudarem nesta etapa.

Aos amigos de mestrado, especialmente ao Micahel e Fernando Otávio, agradeço pelos estudos e ajuda nos momentos mais desesperadores.

Resumo

A criptografia assegura a confidencialidade na troca de arquivos entre as partes envolvidas, sejam elas simples mensagens, áudios, vídeos ou mesmo arquivos mais complexos, mantendo a segurança e o sigilo das informações contidas nesses arquivos. Essa dissertação discute e implementa os métodos RSA e AES de criptografia para sinais de voz. A plataforma MATLAB foi usada para desenvolver os algoritmos e dois tipos de sinais de voz foram usados, a vogal /a/ e a palavra /aui/. Para cada método e para cada tipo de sinal de voz, as etapas de quantização, codificação, criptografia e decifragem foram implementadas. Para a quantização, foram considerados três métodos; quantização uniforme, quantização não-uniforme pela lei μ e quantização não-uniforme pela Lei A. Os resultados obtidos foram analisados e comparados. Um capítulo da dissertação é dedicado a discussão da criptografia quântica. Embora nenhuma implementação tenha sido realizada nesse caso, a sua discussão é importante devido a possibilidade de sua ampla aplicação no futuro.

Palavras-chave: Métodos de criptografia, Criptografia do sinal de voz, método RSA, método AES, criptografia quântica.

Abstract

Encryption ensures confidentiality in the exchange of files between the parties involved, whether simple messages, audio, video, or even more complex files, maintaining the security and confidentiality of the information contained in these files. This dissertation discusses and implements RSA and AES methods to voice files. The Matlab platform was used to develop the corresponding algorithms and two kinds of speech signals are used, the vowel / a / and the word / aui /. For each method and for each type of voice signal, the steps of quantization, encoding, encryption and decryption were implemented. For quantization, three methods were taken into account; uniform quantization, non-uniform quantization by law mu and non-uniform quantization by law A. The results were analyzed and compared. A chapter of the dissertation is devoted to discussion of quantum encryption. Although no implementation has been carried out in this case, its discussion is important because of the possibility of its wide application in the future.

Keywords: Encryption methods, voice signal encryption, RSA method, AES method, quantum encryption.

Lista de Figuras

Lista de Tabelas

Sumário